IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method ~~for tracking entities in a computer network,~~ comprising:

~~a)~~ receiving node information for a node coupled to a computer network;

~~b)~~ determining whether to issue an alarm indicating a network intrusion responsive to receiving the node information by comparing a unique identifier included in said node information to a database ~~determining whether an entity associated with said node has been previously identified in said computer network~~;

~~c)~~ automatically linking at least a portion of said node information to an existing database entry in the database ~~for said entity~~ and not issuing the alarm when the comparison indicates a tracked entity that corresponds to the node ~~if said entity has been previously identified in said computer network~~; ~~and~~

issuing the alarm indicating the network intrusion and creating a new database entry when the comparison indicates that the node is a new entity.

~~d) creating a new database entry for said entity if said node has not been previously identified in said computer network and linking said node information to said new database entry for said entity.~~

2. (Currently Amended) The method of Claim 1, further comprising:

analyzing the node information to select the unique identifier;

wherein the selected unique identifier is not a network address such that a false alarm is not sent regardless of whether the node is subject to dynamic address assignment.

~~wherein said b) comprises:~~

~~b1) determining if a unique identifier from said node information matches a unique identifier for said entity in said database~~.

3. (Currently Amended) The method of Claim 2, wherein the alarm is not issued when the comparison indicates the tracked entity that corresponds to the node regardless of whether the node information identifies an unlisted Internet Protocol (IP) address that is absent from the database at a time that the node information is received.

~~wherein said unique identifier comprises a security identifier~~.

4. (Currently Amended) The method of Claim 3 [[2,]] further comprising:

selecting a security identifier provided by an operating system of the node as the unique identifier when the analysis indicates that the node information includes the security identifier;

selecting a serial number provided by a basic input output system of the node as the unique identifier when the analysis indicates that the node information does not include the security identifier; and

selecting a physical address as the unique identifier when the analysis indicates that the node information does not include either of the security identifier and the serial number. ~~wherein said unique identifier comprises a serial number~~.

5. (Currently Amended) The method of Claim 1, further comprising:

analyzing the node information to select the unique identifier;

wherein the selected unique identifier is not based solely on an IP address such that the determination of whether the alarm is sent is independent of whether the node is subject to static or dynamic address assignment.

~~wherein said b) further comprises determining if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not a unique identifier for said entity in said node information.~~

6. (Currently Amended) The method of Claim 5, wherein the unique identifier is a combination of a physical address and a network address for the node ~~said b) further comprises determining if a IP (Internet Protocol) address from said node information matches a computer name associated with said MAC address in said database~~.

7. (Currently Amended) The method of Claim 1 [[6]], wherein the unique identifier that is compared to the database includes a domain name associated with the node, a computer name associated with the node and one other value associated with the node ~~said b) further comprises determining if a domain name from said node information matches a domain name associated with said MAC address and said computer name in said database~~.

8. (Currently Amended) The method of Claim 7 [[6]], wherein the other value is a security identifier, a serial number or a physical address ~~said b) further comprises determining if an operating system from said node information matches an operating system associated with said MAC address and said computer name in said database~~.

9. (Currently Amended) The method of Claim 8 [[1]], further comprising:

selecting the security identifier for the other value when the security identifier is included in the node information, and when the security identifier is not included in the node information selecting the serial number for the other value, and when neither of the security identifier and the serial number are included in node information selecting the physical address for the other value.

~~wherein said b) further comprises:~~

~~b1) determining if a computer name from said node information matches a computer name in said database; and~~

~~b2) determining if a domain name from said node information matches a domain name associated with said computer name in said database.~~

10. (Currently Amended) The method of Claim 1, wherein said entity is a computer system running a particular operating system.

11. (Original) The method of Claim 1, wherein said entity is a user of said computer network.

12. (Original) The method of Claim 1, wherein said entity is a computer system.

13. (Currently amended) An apparatus comprising: ~~A computer readable medium having stored thereon instructions which, when executed on a general purpose processor, implement a method for tracking entities in a computer network, said method comprising:~~

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

receive node information for a node coupled to a computer network;

analyze identifiers included in the received node information to select a value for comparing to a database that lists tracked entities;

determining whether the node corresponds to one of the tracked entities by comparing the selected value to the database;

when the node corresponds to one of the tracked entities, linking at least a portion of the received node information to an existing entry in the database; and

when the node does not correspond to one of the tracked entities, adding an entry for a new entity to the database and linking the node information to the new entry.

~~a) receiving node information related to a node in a computer network;~~

~~b) uniquely identifying an entity associated with said node information;~~

~~c) linking said node information to said entity if an entry exists in a database for said uniquely identified entity; and~~

~~d) creating a new entry in said database for said entity if no entry exists for said uniquely identified entity and linking said node information to said new entry.~~

14. (Currently amended) The apparatus of claim 13 wherein the selected value is not based on an Internet Protocol (IP) address such the node can be correlated to one of the tracked entities even when the node is subject to dynamic IP address assignment. ~~The computer readable medium of Claim 13, wherein said method further comprises~~:

~~b1) determining if a unique identifier from said information for said node matches a unique identifier in said database.~~

15. (Currently amended) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a security identifier is unavailable. ~~The computer readable medium of Claim 14, wherein said unique identifier comprises a security identifier.~~

16. (Currently amended) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a serial number is unavailable. ~~The computer readable medium of Claim 14, wherein said unique identifier comprises a serial number.~~

17. (Currently amended) The apparatus of claim 13 wherein the selected value is based on a physical address for the node when a different preferred identifier is unavailable. ~~The computer readable medium of Claim 13, wherein said b) of said method further comprises determining if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not a unique identifier of said entity in said node information.~~

18. (Currently amended) The apparatus of claim 13 wherein the selected value is based on both a physical address and a network address when a different preferred identifier is unavailable. ~~The computer readable medium of Claim 17, wherein said b) of said method further comprises determining if a computer name from said node information matches a computer name associated with said MAC address in said database.~~

19. (Currently amended) The apparatus of claim 13 wherein the selected value is either not a network address or is a combination of the network address and a globally unique identifier. ~~The computer readable medium of Claim 18, wherein said b) of said method further comprises determining if a domain name from said node information matches a domain name associated with said MAC address and said computer name in said database.~~

20. (Currently amended) The apparatus of claim 13 wherein the selected value is not based on an IPv4 address such the node can be correlated to one of the tracked entities even when the node is subject to dynamic IPv4 address assignment. ~~The computer readable medium of Claim 19, wherein said b) of said method further comprises determining if an operating system from said node information matches an operating system associated with said MAC address, said computer name, and said domain name in said database.~~

21. (Currently amended) The apparatus of claim 13 wherein the processors are further operable to:

select either a security identifier provided by an operating system of the node or a serial number provided by a basic input output system of the node for the value when the received node information includes either the security identifier or the serial number; and

select a physical address for the value when the received node information does not include either the security identifier or the serial number.

~~The computer readable medium of Claim 13, wherein said b) of said method further comprises:~~

~~b1) determining if a computer name from said node information matches a computer name in said database; and~~

~~b2) determining if a domain name from said node information matches a domain name associated with said computer name in said database.~~

22. (Currently amended) The apparatus of claim 13 wherein the processors are further operable to trigger issuance of an intrusion alarm when the node does not correspond to one of the tracked entities. ~~The computer readable medium of Claim 13, wherein said entity is a computer system running a particular operating program.~~

23. (Currently amended) The apparatus of claim 23 wherein issuance of a false alarm is avoided when the received node information is linked to an existing entry in the database. ~~The computer readable medium of Claim 13, wherein said entity is a user.~~

24. (Currently amended) The apparatus of claim 13 wherein the processors are further operable to use adaptive scanning before determining whether to issue an alarm. ~~The computer readable medium of Claim 13, wherein said entity is a computer system.~~

25. (Currently amended) A method for tracking entities in a computer network comprising:

~~a)~~ receiving node information related to a node on said computer network;

analyzing the received node information to located a unique identifier that is able to uniquely identify said entity, the unique identifier being a value other than a network address for the node;

~~b)~~ determining if a database entry exists for an entity associated with said node by searching said database for the [[a]] unique identifier from said node information ~~that is able to uniquely identify said entity~~, if said unique identifier exits;

~~c)~~ determining if said database entry exists by searching said database using multiple identifiers from said node information that are not able to individually uniquely identify said entity, if said node information does not include said unique identifier;

~~d)~~ linking at least a portion of said node information to said entry if said entry exists; and

~~e)~~ creating a new entry in said database for said entity if no entry exists for said entity, and linking at least the portion of said node information to said new entry.

26. (Original) The method of Claim 25, wherein said multiple identifiers comprise a media access control (MAC) address.

27. (Original) The method of Claim 26, wherein said multiple identifiers further comprise a computer name.

28. (Original) The method of Claim 27, wherein said multiple identifiers further comprise a domain name.

29. (Original) The method of Claim 28, wherein said multiple identifiers further comprise an operating system.

30. (Original) The method of Claim 28, wherein said multiple identifiers comprise at least two of: a media access control (MAC) address, a computer name, a domain name, and an operating system.

31. (Original) The method of Claim 25, wherein said unique identifier comprises a security identifier.

32. (Original) The method of Claim 25, wherein said unique identifier comprises a serial number.

33. (Currently amended) The method of Claim 25, further comprising:

~~f)~~ returning an identifier for an entity in response to a request including a node identifier.

34. (Currently amended) The method of Claim 25, further comprising:

~~f)~~ returning identifiers for all nodes associated with an entity in response to a request including an entity identifier.

35. (Currently amended) The method of Claim 25, further comprising:

~~f)~~ returning node information in response to a request for said node information including a node identifier.

36. (Currently amended) A system for tracking entities in a computer network, comprising:

means for receiving node information related to a node coupled to a computer network;

means for processing the received node information to located a unique identifier that is either not a network address or based on at least one other value in addition to the network address;

means for determining whether an entity associated with said node has been previously identified in said computer network using said unique identifier;

means for linking said node information to an existing database entry for said entity if said entity has been previously identified in said computer network; and

means for creating a new database entry for said entity if said node has not been previously identified in said computer network and linking at least a portion of said node information including the unique identifier to said new database entry for said entity.

37. (Currently amended) The system for tracking entities in a computer network of Claim 36, further comprising means for determining if the [[a]] unique identifier from said node information matches a unique identifier in said database.

38. (Currently amended) The system for tracking entities in a computer network of Claim 36, further comprising means for determining if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not the [[a]] unique identifier in said node information.

39. (Original) The system for tracking entities in a computer network of Claim 36, further comprising means for determining if a computer name from said node information matches a computer name associated with said MAC address in said database.

40. (Original) The system for tracking entities in a computer network of Claim 36, further comprising:

means for determining if a computer name from said node information matches a computer name in said database; and

means for determining if a domain name from said node information matches a domain name associated with said computer name in said database.

41. (Cancelled)

42. (Cancelled)

43. (Currently amended) A system for tracking entities in a computer network, comprising: ~~The system for tracking entities in a computer network of Claim 41,~~

a database storing therein entries related to entities in said computer network;

an engine coupled to said database, wherein said engine is operable to:

receive node information related to a node coupled to said computer network;

determine whether an entity associated with said node has been previously identified in said computer network;

link said node information to an existing entry for said entity in said database if said entity has been previously identified in said computer network; and

create a new entry for said entity in said database if said node has not been previously identified in said computer network and link said node information to said new database entry for said entity;

wherein said engine is further operable to determine if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not a unique identifier in said node information.

44. (Currently amended) The system for tracking entities in a computer network of Claim 43 [[41]], wherein said engine is further operable to determine if a computer name from said node information matches a computer name associated with said MAC address in said database.

45. (Currently amended) The system for tracking entities in a computer network of Claim 43 [[41]], wherein said engine is further operable to determine if a computer name from said node information matches a computer name in said database and determine if a domain name from said node information matches a domain name associated with said computer name in said database.